FORSCOM Policy Memorandum 25-05-01

16 February 2007
Expires: 17 February 2009

AFCI-IC

MEMORANDUM FOR Chiefs, Primary and Special Staff Agencies

SUBJECT: System Administrator Acceptable Use Policy for FORSCOM Command and Control System (FCCS)

1. References:

a. Army Regulation 25-2, Information Assurance, 14 NOV 03.

b. Army Regulation 25-1, Army Knowledge Management and Information Technology Management, 30 Jun 04.

c. Memorandum, DOD CIO, 14 AUG 06, Subject: Approval of the Alternate Logon Token, AKO Document Number: 6197468.

d. Memorandum, DOD CIO, 14 NOV 06, Alternative Smart Card Logon, (ASCL) Token for Two-Factor Authentication.

e. DOD 8570.1M paragraph C3.2.4.2, 15 AUG 04.

f. DOD 8500.2, 6 FEB 03.

2. It is the responsibility of the FORSCOM Deputy Chief of Staff, G-6, Command and Control Support Division (C2SD) to provide operational and maintenance support for all components of the FCCS. To ensure reliability, availability, and supportability of all systems and data on the FCCS network, the following guidelines are issued with regard to System Administrator and User rights for FCCS components.

3. By definition, user rights are rules that determine the action a user can perform on systems supported by the Operating Systems Platform. System Administrators have elevated rights and privileges allowing complete access and authority to the system they administer. Caution is advised when issuing administrative rights, as destruction of network resources may occur with novice or untrained users.

4. Army policy requires that all IT positions be evaluated and a sensitivity level assigned to the position description. Anyone having "root" access shall be designated as IT-I. Other personnel operating/managing network or infrastructure components are designated IT-II positions.

5. The FCCS requires System Administrators to use the Alternative Smart Card Logon (ASCL) for personnel with multiple roles such as system administrators.

6. System Administrator elevated positions and rights are identified as:

a. Organizational Unit (OU) Administrators positions in Active Directory are designated as IT-II. The OU Administrator rights are limited to the G-6, C2SD, Network Services Branch only. The OU Administrator account password will be tightly controlled and issued by signature only from the Information Assurance Security Office (IASO) until use of the Alternative Smart Card Logon (ASCL) is implemented. The ASCL token will allow two factor authentications to be established within Active Directory to support these roles. The Chief, Network Services Branch or his/her designee must approve all OU Administrator accounts.

b. Local Administrators are designated as IT-II. They are members of a workstation local administrators group and have complete authority over the workstation on which the group resides. Local Administrator rights for local workstations are limited to the FCCS Support Team and Information Management Officer (IMO's). In establishing the categories of positions, other factors may enter into the determination, permitting placement in higher or lower categories based on the unique characteristics of the system or the safeguards protecting the system.

c. Developers Group are designated IT-II. Members of the G-6, FORSCOM application team or other such development groups may be granted local administrative rights to their workstations by following procedures for minimum requirements stated in paragraph 5b.

7. Personnel who have privileged access and limited privileged access (IT-I and IT-II) are required to be IA trained, certified. The definition of privileges is:

a. Privileged access. Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network.

b. Limited privileged access. Privilege access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

c. Computing Environment (CE). Workstation or server host and its operating system, peripherals, and applications.

d. Network Environment (Computer). The constituent element of an enclave responsible for connecting CE by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

e. On the job training (OJT). Supervised hands on training based on specific performance criteria that must be demonstrated to a qualified supervisor.

8. All individuals designated as System Administrator (SA), Local Administrators or have elevated privileges will complete technical training within 6 months of assuming position. Individuals performing IA functions must hold, at a minimum, an IA Technical Level I certification, before gaining privileged access to any DOD system. They are designated as IT-II per AR 25-2. SA's and IMO's designated as IT-II shall be fully qualified per DOD Instruction 8500.2, trained, and certified to perform their duties. The minimum training requirement is:

a. IASO course (https://ia.gordon.army.mil) – estimated: 1 hour

b. IA Technical Level 1 course (SkillPort>CIO G-6/NETCOM Information Assurance>Technical Level I Certification -11 modules) – estimated: 5 - 7 days.

c. Network Security Issues (SkillPort>CIO-G6/NETCOM Information Assurance>CIO-G6/NETCOM IA Phase I>Net Safety>Security Issues) – 1 module (estimated: 3.5 hours).

d. Completion of an on-the-job skills practical evaluation to meet functional requirements of DOD 8570.01M. This requirement must be validated by the individual IAPM or IAM.

9. Should the administrator require FCCS support team assistance to rebuild or return a workstation or server to operational status, the local administrative rights may be revoked if it is determined that failure of the Information System was due to negligence. Final authority for revoking user administrative rights is the Designated Approving Authority (DAA). (All exceptions granted to this policy are granted by the DAA).

10. For additional information or assistance, please contact your staff IMO or the FCCS Customer Support Center, (404) 464-2222.

MICHAEL J. FLYNN
Colonel, Signal Corps
FORSCOM, G-6